REMARKS

Claims 1, 18, 35, 36, and 38 have been amended. Claims 37 and 53 have been previously canceled. Claims 1-36, 38-52, and 54 remain pending in the application. Reconsideration is respectfully requested in light of the following remarks.

Section 103(a) Rejections:

The Examiner rejected claims 1-16, 18-33 and 35-53 under 35 U.S.C. § 103(a) as being unpatentable over Hoover (U.S. Patent 5,721,779), and claims 17, 34 and 54 as being unpatentable over Hoover in view of Funk (U.S. Patent 5,721,779). Applicant respectfully traverses these rejections for at least the following reasons.

In regard to claim 1, Hoover fails to teach or suggest *transmitting the response to a remote authorisation unit to authenticate the response without transmitting the pass code to the remote authorisation unit and without generating the pass code from the user input prior to said transmitting*. Hoover's design is based on the goal of protecting a user's PIN from an attacker "as the user inputs the access code, either through software or by physically looking over the user's shoulder", (column 2, lines 65 - 68), wherein the software "collects, and saves to a file, all the keystrokes that the user types on his keyboard", (column 1, lines 25 and 26) and/or captures "the locations … of mouse clicks and [uses] them to deduce the characters indicated", (column 1, lines 36 - 38). Hoover describes a system for hiding user input (e.g., PIN numbers or passwords) by displaying pseudo-randomized characters and allowing the user to change (e.g., increment and decrement) the characters until the access code is displayed. Hoover does not protect the PIN during transmission, rather Hoover protects the PIN at the time of input. Column 3, lines 16-19 state, "Based on the display, the user provides feedback (in the form of an entered access code) via input device 340, which is passed back through processor 320 to access control program 350." Note that Hoover passes the actual access code (i.e., password) to local processor 320 for validation. Hoover clearly teaches that the PIN is generated in column 2, lines 56-63 which state, "The user would input to an adjacent row

an offset digit sequence such that the correct PIN digit sequence was formed when the offset digit sequence row was added to the initially random PIN digit sequence row. The resulting correct PIN digit sequence could be displayed adjacent to the other two rows." In contrast, Applicant's claim requires transmitting the response (e.g., the transformation of the challenge) received from the user input device to a remote authorization unit without including the pass code and without the pass code having even been generated.

Hoover also discloses sending the PIN in an Internet environment. Column 3, lines 30-40 states,

> In an Internet environment, the user-selectable fields could be implemented (i) using Javascript on a web page to send the PIN to a common gateway interface (CGI) script or active server page, (ii) using a Java applet on a web page to send the PIN to a CGI script or active server page, (iii) using a plug-in with a GUI on a web page to send the PIN to a CGI script or active server page, (iv) using a specialized network application with a GUI to send results by a network connection to a server application, or (v) using a specialized network application with command line input.

Thus, Hoover clearly sends the actual PIN (or pass code) in all embodiments. In contrast, Applicant's claim requires that the response be sent without the pass code and without generating the pass code from the response.

In the Office Action dated July 31, 2008, the Examiner states it would be obvious to transmit the offset digit sequence without transmitting the actual pass code. However, the Examiner's unfounded speculation is counter to the explicit teachings of Hoover. As shown above, Hoover states that the action of adding the initially random and user inputted offset digit sequences produces the actual PIN that is stored and available for transmission. In the internet environment described in Column 3, lines 30-40, the actual PIN is transmitted to the server via a Javascript or a Java applet on a web page, or a GUI plug-in, or a specialized network application; all of which produce user-selectable fields and occur at the client. Thus the actual PIN is generated and stored on the client and then transmitted. Also, in Hoover the server or other recipient is not stated to have any knowledge of the initially random digit sequence, and therefore would not be capable of validating the request unless the actual pass code is transmitted. Also, note that claim not

only says that the response is transmitted without the pass code, but also without even generating the pass code from the user input prior to said transmitting. This is explicitly not the case in Hoover.

Thus, for at least the reasons presented above, the rejection of claim 1 is not supported by the cited art and removal thereof is respectfully requested. Similar remarks as those above regarding claim 1 also apply to claims 18, 35, and 38.

Regarding claim 17, Hoover in view of Funk fail to disclose, *using the response to encrypt said communications challenge; and transmitting the encrypted communications challenge to the authorisation unit; thereby allowing the response to be validated by said authorisation unit using said stored data record of, the pass code*. The Examiner admits Hoover fails to teach using the response to encrypt the communications challenge and relies on Funk, citing column 4, lines 50-52. Funk is directed towards utilizing a challenge and response handshake to allow a server to authenticate a client based on a password. Column 4, lines 50-53 state, "The client can generate this response signal by employing the same one-way commutative function to encrypt the challenge signal, C, with one valid password." Funk uses the actual password to generate the response. Column 4, line 59 provides the following formula: Response=$F(C,$ Password)=C^{password} mod q. In contrast, Applicant's claim requires using the response (e.g., transformation of the challenge), not the actual pass code, to encrypt the communications challenge. Both Hoover and Funk use the actual PIN or password in their respective designs. Thus, Funk combined with Hoover would not result in Applicant's claimed invention.

Thus, for at least the reasons presented above, the rejection of claim 17 is not supported by the cited art and removal thereof is respectfully requested. Similar remarks as those above regarding claim 17 also apply to claims 34, and 54.

Applicant asserts that the Examiner has not stated a proper *prima facie* rejection of claim 36. The Examiner rejected claim 36 along with claims 18 and 38. Applicant notes that the limitations of claim 36 differ in scope from the limitations of claims 18 and 38. **Since the actual limitations of claim 36 have not been addressed, no *prima facie* rejection has been stated for this claim.**

In further regard to claim 36, Hoover does not teach or suggest *receiving, from a user-input device, user input capable of transforming the challenge into a pass code allocated to the user, wherein the user input is dependent on the challenge such that the user input capable of transforming the challenge into the pass code is different for different challenges; generating a response from the user input received from the user input device, wherein the response is not the pass code; generating a predicted response based on knowledge of the challenge and a stored version of the pass code; and validating the user on the basis of said response compared to the predicted response, wherein neither the response nor the predicted response is the pass code*. As discussed above, the actual password or PIN is generated, transmitted and used for validation in Hoover's design. Hoover does not teach or suggest generating a predicted response based on knowledge of the challenge and a stored version of the pass code; and validating the user on the basis of said response compared to the predicted response, wherein neither the response nor the predicted response is the pass code.

Applicant also asserts that the rejections of numerous ones of the dependent claims are further unsupported by the cited art. However, since the rejections have been shown to be unsupported for the independent claims, a further discussion of the dependent claims is not necessary at this time.

CONCLUSION

Applicant submits the application is in condition for allowance, and notice to that effect is respectfully requested.

If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/5681-74900/RCK.

Respectfully submitted,

/Robert C. Kowert/
Robert C. Kowert, Reg. #39,255
Attorney for Applicant

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: October 31, 2008